Date: February 15, 2000 DSL-BQA 00-014

To:		
	Adult Day Care	ADC - 02
	Adult Family Homes	AFH - 04
	Ambulatory Surgery Centers	ASC - 02
	Certified Mental Health and AODA Programs	CMHA - 02
	Community Based Residential Facilities	CBRF - 05
	Outpatient Rehabilitation Facilities (including Comprehensive)	OPRA - 02
	End-Stage Renal Dialysis Centers	ESRD - 02
	Facilities for the Developmentally Disabled	FDD - 04
	Home Health Agencies	HHA - 04
	Hospices	HSPCE - 03
	Hospitals	HOSP - 06
	Nursing Homes	NH - 06
	Residential Care Apartment Complexes	RCAC - 03
	Rural Health Clinics	RHC - 03

From: Susan Schroeder, Director
Bureau of Quality Assurance

Disposal of Medical Records

This memo provides information about new statutory requirements governing the disposal of medical and other records containing personal information, passed as part of the 1999 state budget bill. This law has implications for health care providers that create, receive, retain, and dispose of medical information about their patients or clients. The memo summarizes the provisions of the new law and highlights issues pertaining to health providers that report protected information to the Bureau of Quality Assurance. The memo does not provide authoritative information regarding the interpretation of the law or compliance with it.

Questions about the information in this memo may be directed to the following contact persons:

Nursing Homes, Community Based Residential Facilities, Adult Family Homes, Adult Day Care Centers and Facilities for the Developmentally Disabled should contact their Regional Office:

Southern Regional Office
3514 Memorial Drive
Madison, WI 53704-1162

Phyllis Tschumper, RFOD (608) 243-2374
FAX: (608) 243-2389

Southeastern Regional Office 819 N. 6th St., Rm. 875 Milwaukee, WI 53203-1606	Tony Oberbrunner, RFOD FAX: (414) 227-4139	(414) 227-4908
Northeastern Regional Office 200 N. Jefferson St., Suite 211 Green Bay, WI 54301-5182	Pat Benesh, RFOD FAX: (920) 448-5254	(920) 448-5249
Northern Regional Office 1853 N. Stevens Street P.O. Box 1246 Rhinelander, WI 54501-1246	Marianne Missfeldt, RFOD FAX: (715) 365-2815	(715) 365-2802
Western Regional Office 610 Gibson St. Eau Claire, WI 54701-3667	Joe Bronner, RFOD FAX: (715) 836-2535	(715) 836-4753

All Other Providers Should Contact:

Health Services Section 1 W. Wilson Street P.O. Box 2969 Madison, WI 53701-2969	Section Chief FAX: (608) 266-1518	(608) 266-8084

Background and Purpose of the New Law

Section 3113n of the State budget bill added a new section (895.505) to Chapter 895 of the Wisconsin Statutes. Section 895.50 of the statutes establishes a general right of privacy. Subsection 895.50(2), in particular, defines an invasion of privacy as any "intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private …" It does not, however, specify the categories or forms of personal information that are to be considered private--with the exception of one's name, portrait, or picture--nor does it allow for the imposition of civil or criminal penalties. The new statutory provision addresses an apparent weakness in the existing law created by the clause in subsection 895.50(2), namely that there can be no reasonable expectation that records or other material containing personal information disposed of in a common, public manner or place ("dumpsters," for example) will be protected from deliberate or inadvertent recovery and misuse. Section 895.505 both specifies the types of information that are legally protected and creates a requirement that entities possessing protected information safeguard it from invasions of privacy by taking action to remove or otherwise make unavailable the personally identifiable information or characteristics prior to disposing of it. The law also allows for recovery of damages from and the imposition of civil forfeitures against businesses that improperly dispose of covered records and individuals who obtain and use such records in violation of the law. Individuals who violate the law by retrieving and/or misusing such records ("dumpster divers") may also be subject to imprisonment.

Definitions

Records containing Personally Identifiable Information

Section 895.505 defines a *record* as any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or preserved, regardless of its physical form or characteristics. This clearly includes official and unofficial paper documents as well as computer media that replicate or permit the creation of paper documents.

Section 895.505 defines *personal information* as any of the following:

1. Personally identifiable data about an individual's medical condition, if the data are not generally considered to be public knowledge;
2. Personally identifiable data that contain an individual's financial information that relate to the individual's account(s) or transactions with a financial institution;

3. Personally identifiable data provided upon opening an account with a financial institution or applying for a loan;
4. Personally identifiable data about an individual's tax returns.

Under the law, information is *personally identifiable* if it is possible to associate it with a particular individual through one or more identifiers (for example, name or Social Security Number) *or other information or circumstances*. This means that it is not necessary that the information actually contain a personal identifier, if the other data contained in the record, by itself or in combination with other sources of information, would permit an individual's identity to be deduced.

Disposal

Section 895.505 does not specifically define the actions that constitute disposal of a record or other information, except to state that disposal "does *not* include a sale of a record or the transfer of a record for value" (emphasis added).

Covered Entities

Section 895.505 applies to several entities, including financial institutions, investment companies, tax preparation businesses, and "medical businesses." A medical business is defined as "any organization or enterprise operated for profit or not for profit … that possesses information, other than personnel records, relating to a person's physical or mental health, medical history or medical treatment." It is important to note that possession of information is all that is required under the law; an entity need not have created the record in order to be obligated to protect it or otherwise be covered by the law.

What the Law Requires

In order to protect personal information from improper disclosure and potential misuse, the new law requires any covered business entity that disposes of a covered medical or financial record to first take action to prevent the acquisition and misuse of the personal information that the record may contain. Specifically, the law requires covered business entities to take at least one of the following steps prior to disposing of covered records:

1. Shred the entire record.
2. Erase the personal information contained in the record.
3. Modify the record to make personal information contained in it unreadable.
4. Take action to ensure that no unauthorized person will have access to the personal information contained in the record from the time it is disposed of until the time it is ultimately destroyed.

If a covered business entity disposes of a record containing personal information without taking one or more of these actions, it is liable to the subject of the record for any damages arising from its failure to take such action, and the business may also be subject to a civil forfeiture of up to $1,000. Note that the law does not state that personal information must actually be obtained and misused by an unauthorized individual before a covered business entity may be held liable; the failure to take one or more of the required actions could be sufficient basis on which to impose a civil forfeiture.

Recommendations

Most if not all of the health facilities and providers regulated by the Bureau of Quality Assurance maintain patient or client records that contain the kind of information that is protected under this law. Some providers, notably nursing homes and home health agencies, are required to submit to the Bureau patient records that contain both confidential health information and personal identifiers such as Social Security Numbers. All providers should ensure that they have policies and procedures in place to protect such records from any unauthorized disclosure and use, whether or not it results from "disposal" of the kind envisioned by this new law. At a minimum, this means restricting access to records to staff whose responsibilities require them to have this information, and ensuring that the status and location of all paper or electronic copies of records are known from the time they are received or created until they are destroyed. In particular, it is important to ensure proper control over computer media such as diskettes that may contain copies of records that are also maintained in paper files. Nursing homes and home health agencies that submit patient assessment data to the state, for example, frequently store records containing this data in temporary files on computer hard drives or diskettes, as well as in a master database. While access to the database may be restricted, the temporary storage media may be readily accessible, which could lead to unauthorized or inadvertent copying or disposal of protected information. These providers should ensure that once the required records have been submitted to the state, they are promptly and permanently erased from any computer media used to store them prior to transmission, unless access to such media and the records they contain is controlled at all times.

Other questions about this new law remain to be answered through the process of administrative implementation and possible interpretation by the courts. Among these are what actions on the part of a medical provider or other covered entity constitute "disposal" of a protected record, what standards of completeness or permanence will be applied in determining whether shredding of paper records or erasure of computer files was adequate to meet the law's requirements, and precisely what elements of medical record will be considered protected personal information. In the meantime, providers are urged to adopt a conservative approach to the retention, availability, and disposal of all potentially sensitive medical and personal information, and to remain cognizant of other, possibly more stringent state and federal laws governing patients' privacy and the protection of their personal information.